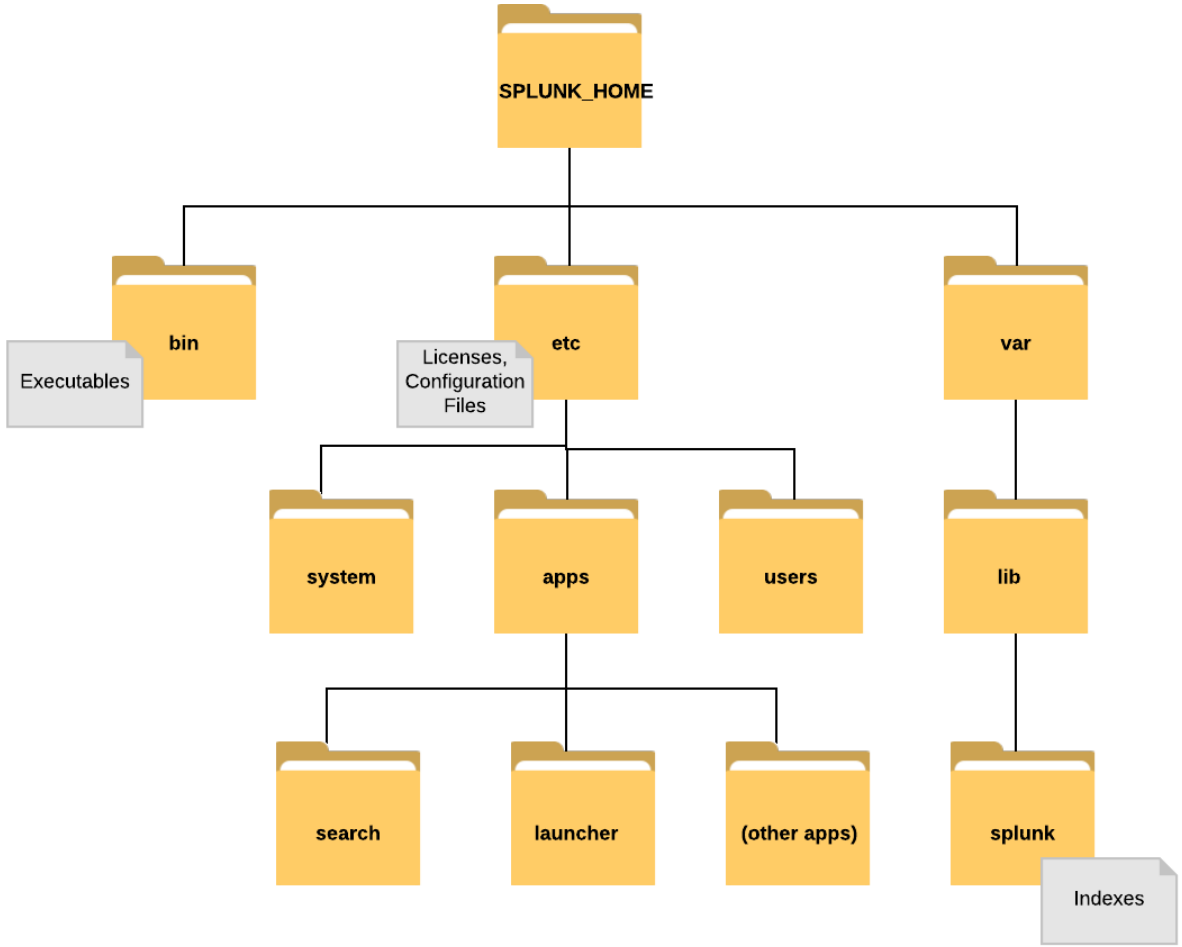
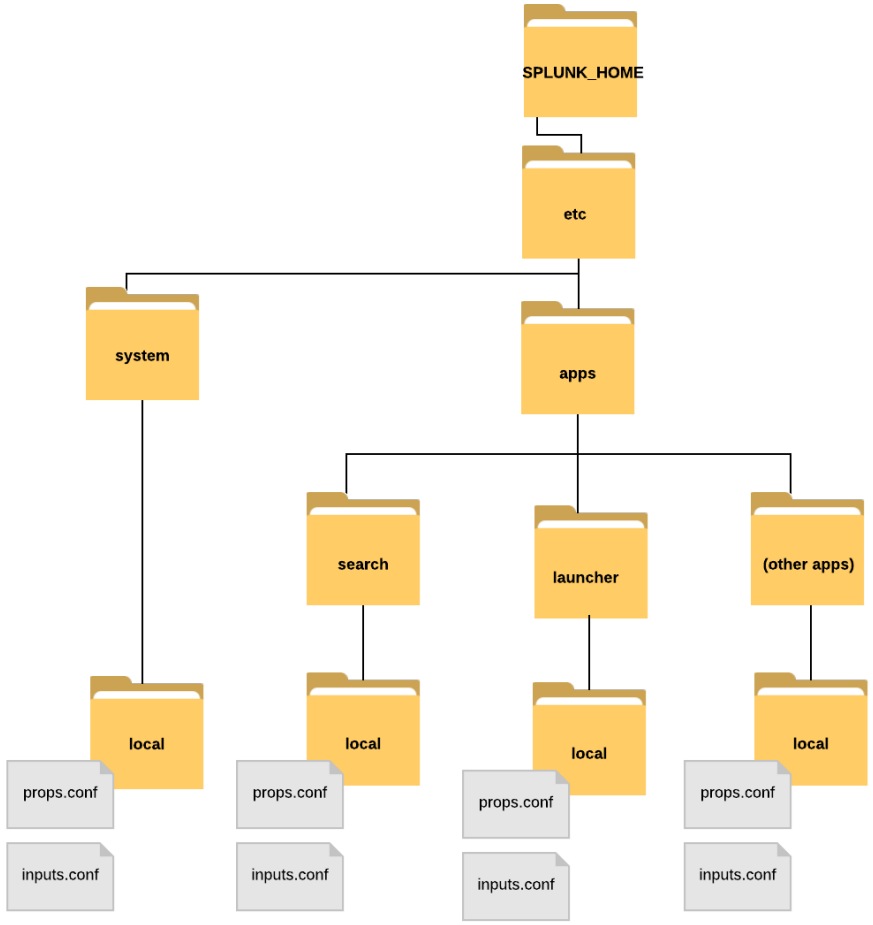
Splunk Configuration Files>

- Govern almost every aspect of how Splunk behaves.
- Are Linux-like, but can be used in Windows (ending in `.conf`)
- Are multi-layered

Splunk Configuration Files>



Splunk Configuration Files>



Same file names

Splunk Configuration Files>

Configuration file structure

- Build on stanzas (sections)

[Stanza Header]

Attributes

```
[stanza_header1]
attribute1 = value
attribute2 = value

[stanza_header2]
attribute1 = value
attribute2 = value
```

Splunk Configuration Files>

Configuration file structure

- Example `outputs.conf`

[Stanza Header]

Attributes

```
[tcpout:splunk_indexer]
Server = 192.168.1.45:9997
```

Splunk Configuration Files>

- Configuration files in the `/default` directories come with Splunk and have default settings.
- Specific changes/configurations should be made in the `/local` directory.

Splunk Configuration Files>

- When Splunk starts, configuration files are *merged* into a single runtime model.
  - If there are no duplicate stanzas, the resulting runtime model is the union of all files.
  - If there are conflicts, the setting with the highest precedence is used.

Splunk Configuration Files>

Precedence

1. System `/local` directory
2. App `/local` directories
3. App `/default` directories
4. System `/default` directory

Splunk Configuration Files>

Important configuration files

File	Purpose
Inputs.conf	Defines data inputs
Outputs.conf	Defines forwarding behavior
Props.conf	Indexing property configurations, custom source type rules, and more!
Limits.conf	Defines various limits for search commands

Thanks, Splunkers!